# Building a Library for Microelectronics Verification with Topological Constraints


***Leleia A. Hsia***
513th Electronic Warfare Squadron
Eglin AFB, FL 32542
Leleia.Hsia.2@us.af.mil

***Graziano Vernizzi***
Dept. of Physics
Siena College
Loudonville, NY 12211
gvernizzi@siena.edu

***Mary Y. Lanzerotti***
Dept. of Physics
Augsburg College
Minneapolis, MN 55454
lanzerot@augsburg.edu

***Derrick Langley***
Air Force Space Command
Los Angeles AFB, CA 90245
Derrick.Langley@us.af.mil



**Abstract:** *This paper proposes a methodology to build a library for gate-level microelectronics verification with topological constraints. Circuits at the second level of abstraction are selected from prior work on simulated reverse-engineered hardware. We show that when signal pairs are switched while maintaining circuit functionality, the topological genus varies according to a frequency distribution that differs for each circuit.*



**Keywords:** Abstraction, Euler characteristic, genus, microelectronics verification, SCR, DARPA TRUST.


## Introduction

The problem of hardware that might contain malicious circuitry or defects has gained significant attention within the Department of Defense (DoD) within the past two and a half decades [1-11]. Hardware that may compromise national security systems must be detected and prevented from entering DoD systems. The Defense Advanced Research Project Agency (DARPA) Trusted Integrated Circuits (TRUST) [12-14] program was introduced to focus on verification and detection of tampering. Our prior work developed a technique to detect altered or additional circuits that do not affect logic [15,16]. Standard cell recognition (SCR) software demonstrated a 90% success rate of perfectly performing SCR on circuits containing 650 transistors [17,18].

## Topological Constraints and Methodology

A circuit at any level of abstraction can be represented as a *combinatorial map* [19, 20] (for a review see [21]). Such a representation is based on a two-dimensional projection of the circuit onto a plane. While there are infinite ways to project the circuit onto a plane, the connectivity between different circuit elements (among terminal vertices, gate vertices, and net vertices) does not vary under 2D projections. The collection of vertices and connections (edges) generate a graph naturally. In particular, a combinatorial map describes any circuit diagram that has been projected onto a 2D surface by using 1) a list of half-edges $D$, 2) a permutation involution $\alpha$ on $D$ with no fixed points, and 3) a shift-permutation $\sigma$ on $D$. The half-edges can be labeled with distinct consecutive integers $[1,..,2m]$ (where $m$ is the number of edges). The $\alpha$ permutation associates each half-edge $i$ to the corresponding half-edge $\alpha(i)$. Obviously, it is an involution, $\alpha(\alpha(i))=i$ (meaning that if the half-edge $i$ is connected to the half-edge $j=\alpha(i)$ then the half-edge $j$ is connected to the half-edge $i$) , and without fixed points, $\alpha(i)\neq i$ (no edge is made of just a single half-edge). The shift permutation $\sigma$ associates each half-edge $i$ to the half-edge $\sigma(i)$ that is to the right of $i$ when turning counterclockwise around the common incident vertex (for netlist vertices and gate vertices), or turning clockwise (for terminal vertices on the external boundary of the circuit). Such a representation fully encodes the connectivity information of the various circuit elements, independently from the 3D embedding. A famous theorem by Euler allows the determination of the *Euler characteristic* of a closed surface on which the schematics can be drawn without crossing connections:

$$\chi=c(\sigma)-c(\alpha)+c(\sigma*\alpha) \qquad (1)$$

where $c(p)$ indicates the number of cycles of the permutation $p$ (every permutation can be decomposed into a set of cycles; a cycle being a sequence of labels that are mapped into each other cyclically). Moreover, $\chi=2-2g$ where $g$ is the topological genus of the circuit (i.e. the number of handles). The calculation of the topological genus of a circuit can be conveniently implemented in MATLAB (Mathworks). We wrote a program to evaluate formula (1) by computing the number of cycles of the permutations $\sigma$, $\alpha$, and $\sigma*\alpha$. The pseudocode we implemented is (for details see [22]):

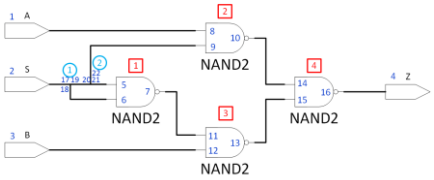
**1.** Given a permutation $P$, set $C$=0
**2. while** the largest element x in P is positive:
**3** Increase $C \rightarrow C=C+1$
**4.** Move to the next element $x \rightarrow P(x)$. Label x as visited by the cycle C, by setting $P(x)=-C$. Repeat step 4 until the next element $P(x)$ is positive (if it is negative, it means that the element has been visited by the cycle $C$ already).
**5. end while** loop
**6.** Output=$-P$, gives the cycles decomposition of $P$

The genus is obtained from the Euler characteristic ($g=1-\chi/2$). The number of edges E is given by $c(\alpha)$. The total number of blocks B=G+N is given by $c(\sigma)$-1 (where the 1 indicates the external boundary, G is the gate count and N is the net count). The number of faces (or loops) is $F=c(\sigma*\alpha)$.

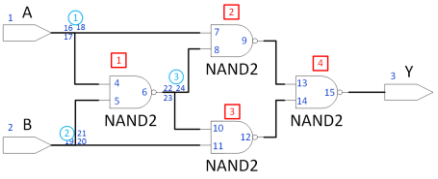
## Preliminary Library

Of the five proposed circuits in Table 1, (a)-(d) are adapted from [18].

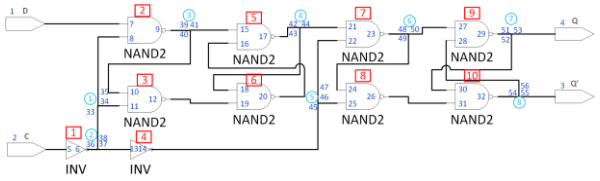
**Table 1**. Schematics for a (a) 2-to-1 MUX; (b) XOR gate; (c) Master Slave Flip Flop (FF); (d) Partial full adder cell; (e) 1-bit full adder cell.



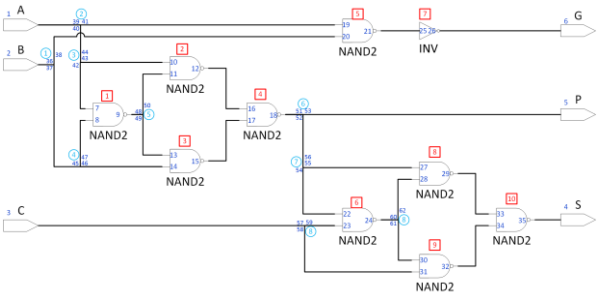

(a) 2-to-1 MUX at second level of abstraction (g=0)



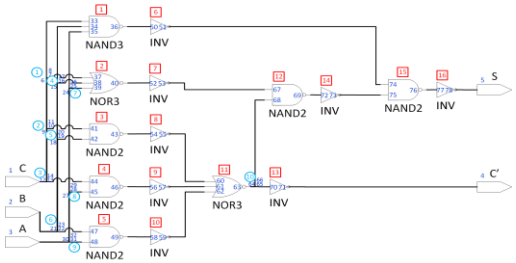

(b) XOR gate at second level of abstraction (g=0)




(c) Master Slave FF at second level of abstraction (g=2)




(d) Partial full adder cell at 2nd level of abstraction (g=1)




(e) 1-bit full adder cell, adapted from [23] (g=5)

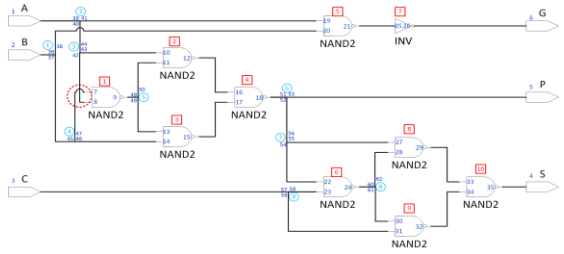
The circuits in Table 1 are composed of basic CMOS gates that typically comprise books in random logic and semi-custom design methodologies in high-performance microprocessor design [24, 25]. Table 1 shows schematics with no switched signals of a (a) 2-to-1 MUX; (b) XOR gate; (c) Master Slave Flip Flop; (d) Partial full adder cell; (e) 1-bit full adder cell. Net, gate, and terminal vertices are labeled with blue circles, red squares, and digits, respectively. Table 2 shows corresponding topological constraints.

**Table 2**. Topological constraints for the library circuits in Table 1.

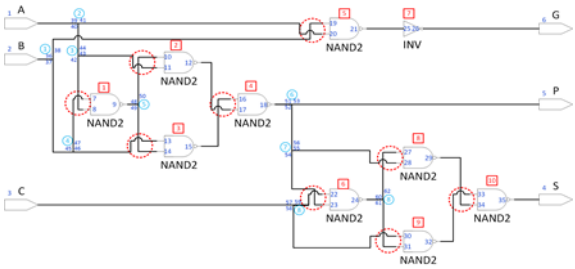
| **Circuit. Note that c = 1** [26] | **Topological Constraints** [27] **{G,N,T,B,g,χ,F,E}** | **Schematic Braid Words** [27] |
|---|---|---|
| **2-to-1 MUX** | {4, 2, 4, 6, 0, 2, 6, 11} | $\sigma^{\pm1.0}_{5,6}\sigma^{\pm1.0}_{8,9}\ \sigma^{\pm1.0}_{11,12}\ \sigma^{\pm1.0}_{14,15}$ |
| **XOR gate** | {4, 3, 3, 7, 0, 2, 6, 12} | $\sigma^{\pm1.0}_{4,5}\ \sigma^{\pm1.0}_{7,8}\ \sigma^{\pm1.0}_{10,11}\ \sigma^{\pm1.0}_{13,14}$ |
| **Master Slave Flip Flop** | {10, 8, 4, 18, 2, -2, 7, 28} | $\sigma^{\pm1.0}_{7,8}\ \sigma^{\pm1.0}_{10,11}\ \sigma^{\pm1.0}_{15,16}\ \sigma^{\pm1.0}_{18,19}$ $\sigma^{\pm1.0}_{21,22}\ \sigma^{\pm1.0}_{24,25}\ \sigma^{\pm1.0}_{27,28}\ \sigma^{\pm1.0}_{30,31}$ |
| **Partial full adder cell** | {10, 9, 6, 19, 1, 0, 11, 31} | $\sigma^{\pm1.0}_{7,8}\ \sigma^{\pm1.0}_{10,11}\sigma^{\pm1.0}_{13,14}$ $\sigma^{\pm1.0}_{16,17}\sigma^{\pm1.0}_{19,20}\ \sigma^{\pm1.0}_{22,23}\sigma^{\pm1.0}_{27,28}$ $\sigma^{\pm1.0}_{30,31}\ \sigma^{\pm1.0}_{33,34}$ |
| **1-bit full adder cell** | {16,10,5,26,5,-8,4, 39} | 1 (no switches) |

Table 3 shows two topological representations for a partial full adder cell with (a) one switched signal pair (g=2), and (b) nine switched signal pairs (g=4). Note that 7 crosses above 8 in Fig. 1(a).

**Table 3**. Partial full adder cell with (a) one switched signal pair in red (g=2) compared with Table 1(d); (b) nine switched signal pairs circled in red (g=4) compared with Table 1(d).




(a)




(b)

## Frequency Distributions

Table 4 shows the average genus and mode for four circuits when each signal pair is switched.

**Table 4**. Average genus, *g*, with switched pairs in library circuits.

| (a) 2-to-1 MUX | | | (b) XOR Gate | | |
|---|---|---|---|---|---|
| **Pair** | **Average *g*** | **Mode** | **Pair** | **Average *g*** | **Mode** |
| **[5,6]** | 1.750 | 2 | **[4,5]** | 1.875 | 2 |
| **[8,9]** | 1.750 | 2 | **[7,8]** | 1.750 | 2 |
| **[11,12]** | 1.625 | 2 | **[10,11]** | 1.750 | 2 |
| **[14,15]** | 1.625 | 2 | **[13,14]** | 1.625 | 2 |
| **no switches** | 0 (Table 1a) | n/a | **no switches** | 0 (Table 1b) | n/a |
| **(c) Master Slave FF** | | | **(d) Partial Full Adder Cell** | | |
| **Pair** | **Average *g*** | **Mode** | **Pair** | **Average *g*** | **Mode** |
| **[7,8]** | 3.773 | 4 | **[7,8]** | 4.188 | 4 |
| **[10,11]** | 3.594 | 4 | **[10,11]** | 4.125 | 4 |
| **[15,16]** | 3.539 | 4 | **[13,14]** | 4.125 | 4 |
| **[18,19]** | 3.328 | 4 | **[16,17]** | 4.063 | 4 |
| **[21,22]** | 3.672 | 4 | **[19,20]** | 4.000 | 4 |
| **[24,25]** | 3.734 | 4 | **[22,23]** | 4.281 | 4 |
| **[27,28]** | 3.484 | 4 | **[27,28]** | 4.156 | 4 |
| **[30,31]** | 3.484 | 4 | **[30,31]** | 4.156 | 4 |
| **n/a** | n/a | n/a | **[33,34]** | 4.031 | 4 |
| **no switches** | 2 (Table 1c) | n/a | **no switches** | 1 (Tables 1d, 3b) | n/a |

Table 5(a)-(d) and Fig. 1 show frequency distributions for the 2-to-1 MUX (Table 1a); XOR Gate (Table 1b); Master Slave Flip Flop (Table 1c); partial full adder cell (Tables 1d, 3b); 1-bit full adder cell (Fig. 1), respectively.

**Table 5**. Frequency distributions for the genus of logically equivalent circuit topologies for (a) 2-to-1 MUX (16); XOR gate (16); (c) Master Slave Flip Flop (256); and (d) partial full adder cell (512).

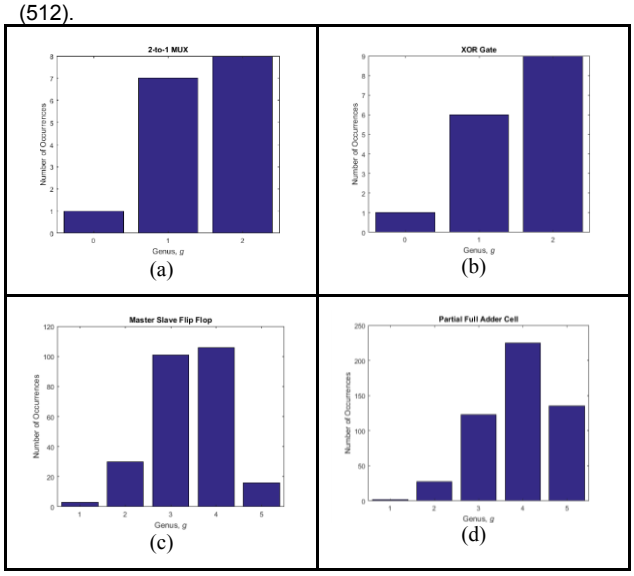



Figure 1 shows that switching signal pairs produces logically-equivalent topologies of the 1-bit full adder cell with three values of the genus (g = 3 [1 case], 4, 5, 6).

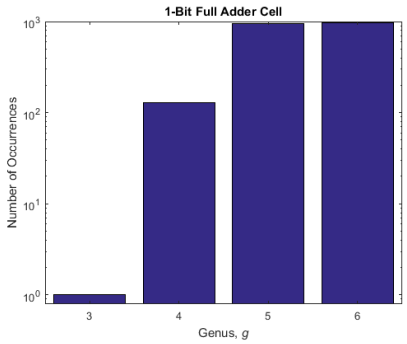



**Figure 1**. Frequency distribution for logically equivalent circuit topologies of the 1-bit full adder cell (2048) in Table 1(e) for non-overlapping switches [41,42];[44,45];[47,48];[67,68];[74,75];[33,34]; [34,35];[35,33];[37,38];[38,39];[39,37];[60,61];[61,62];[62,60].

## Discussion

It is important to emphasize that a given circuit can be drawn on a plane in many ways, depending on how the 2D projection is performed. An analogy can be made by considering different projections on a plane of a three-dimensional knot. While different planar projections look different, the knot is still the same. Analogously, the circuit functionality is determined *uniquely* by the specific connectivity of its elements, and the actual 2D schematic is only one of many possible representations. The topological genus *g* is a quantity that is capable of capturing the complexity of the circuit connectivity, which is completely independent from the chosen planar projection for the schematic, i.e. *any* different schematics of the *same* circuit will give the same topological genus *g*. It is shown here for the first time that by exploring the space of different circuits, all having the same functionality (iso-functional), the genus fluctuates in a fashion that is characteristic of the circuit itself, and therefore in a fashion that is characteristic of its functionality. Such a concept has been explored extensively in biology for the study of neutral mutations of DNA sequences (also known as *silent* mutations). Such mutations do not significantly alter the characteristics of the organism (i.e. its functionality) and therefore its fitness. We apply a similar approach to the study of a circuit with a given functionality, and the space of iso-functional circuits.

## Future Work

Future work will add capabilities to switch additional signals (See, for example, signals [6,8] and [16,18] in Fig. 2) and represent electrical properties of a physical design layout [28].

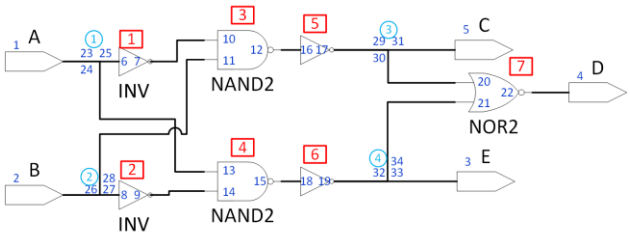



**Figure 2**. Digital comparator.

## Acknowledgments

GV and ML thank Sam Swanson, University of Minnesota Mankato, for assistance with Table 1(e). ML thanks the Department of Electrical and Computer Engineering at the University of Minnesota. ML thanks Air Force Institute of Technology (AFIT) and Dr. Adedeji Badiru, Dean at AFIT, for support of this research.

## References

1. *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*. [Online]. Tech. Rep., U.S. Senate Committee on Armed Services, May 2012. Available: http://www.armed-services.senate.gov/imo/media/doc/ Counterfeit-Electronic-Parts.pdf.
2. M. Pecht and S. Tiku, "Bogus!". [Online]. *IEEE Spectrum*, 1 May 2006. Available: http://spectrum.ieee.org/computing/hardware/bogus
3. E. Savitz, "The Serious Risks From Counterfeit Electronic Parts". [Online]. *Forbes*, 11 July 2012. Available: http://www.forbes.com/sites/ ciocentral/2012/07/11/the-serious-risks-from-counterfeit-electronic-parts/
4. "Trusted Integrated Circuits (TRUST)". [Online]. DARPA Microsystems Technology Office. Available: http://www.darpa.mil/Our_Work/MTO/Programs/Trusted Integrated Circuits (TRUST).aspx
5. D. Collins, "DARPA "TRUST in IC's" Effort" [Online]. 2007. Available: http://www.dtic.mil/docs/citations/ADA503809. DARPA Microsystems Technology Symposium.
6. "Want to See Some "Fake" Microelectronics?". NAVSEA Warfare Centers, DARPA MTO Exposition, 18 July 2014.
7. D. Evans, "Understanding and Mitigating Supply Chain Risks for Computing and Communications (or: Who's Driving Your Missiles?)." Technical report, DARPA Defense Sci. Study Group.
8. Y. Li, R. Iskander, and M.-M. Louerat, "Modeling, design and verification platform using SystemC AMS". *2014 15th Intl. Symposium on Quality Electronic Design*, 39–46. 2014.
9. C. Liang, "Mixed-signal verification methods for multi-power mixed-signal System-on-Chip (SoC) design". *2013 IEEE 10th International Conference on ASIC*, 1–4. 2013.
10. M. Beaumont, B. Hopkins, and T. Newby, *Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review). Technical report, Command, Control, Communications and Intelligence Division, Defence Science and Technology Organisation,* Australian Department of Defence, Jul 2011.
11. M. Bezerra, A. Oliveiray, and P. Adeodato, "Predicting software defects: A cost-sensitive approach," *2011 IEEE Intl. Conference on Systems, Man, and Cybernetics (SMC)*, 2515-2522. 2011.
12. Dean R. Collins, "TRUST, A Proposed Plan for Trusted Integrated Circuits," ADM202011, GOMACTech-06, San Diego, CA, March 20-23, 2006. Online. Available: http://ece-research.unm.edu/jimp/HOST/govt_reports/dean_collins_paper.pdf.
13. *Defense Science Board Task Force on High Performance Microchip Supply*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC. February 2005. Online. Available: http://www.acq.osd.mil/dsb/reports/ADA435563.pdf.
14. James R. Gosler, *The Digital Dimension*, in "Transforming US Intelligence", Edited by Jennifer E. Sims, Borton Gerber, Georgetown University Press, p. 106, 2005.
15. M. Seery, *Complex VLSI Feature Comparison For Commercial Microelectronics Verification*. Master's Thesis, Air Force Institute of Technology, WPAFB, OH, 2014.
16. M. Seery, M. Lanzerotti, and L. Orlando, "Complex VLSI Feature Comparison For Commercial Microelectronics Verification*," 39th GOMAC,* 2014.
17. L. A. Hsia, D. Langley, M. Seery, M. Lanzerotti, and L. Orlando, "Standard Cell Recognition for Gate-Level Commercial Microelectronics Verification," *40th GOMAC,* 2015.
18. L. A. Hsia*, "Standard Cell Recognition for Gate-Level Commercial Microelectronics Verification."* Master's Thesis, Air Force Institute of Technology, WPAFB, Ohio, 2015.
19. Jacques A., Constellations et Graphes Topologiques, Colloque Math. Soc. János Bolyai, p. 657-672, 1970.
20. Ringel G., *Map Color Theorem*, Springer-Verlag, Berlin 1974.
21. J. Bouttier, "Matrix integrals and enumeration of maps," in *Oxford Handbook of Random Matrix Theory*, Ed., 2011.
22. G. Vernizzi, H.Orland, and A. Zee, Classification and predictions of RNA pseudoknots based on topological invariants, *Phys. Rev. E,* vol. 94, 042410, 2016.
23. F. P. Preparata, *Introduction to Computer Engineering*. New York: John Wiley & Sons, Inc., 1985.
24. G. A. Northrop, P.-F. Lu*,* "A Semi-Custom Design Flow in High-Performance Microprocessor Design," *Design Automation Conf.,* Paper 27.2, Las Vegas, NV, 2001.
25. P.-F. Lu, G. A. Northrop, K. Chiarot, "A Semi-custom Design of Branch Address Calculator in the IBM Power4 Microprocessor," *VLSI Design and Test Conf.,* pp. 329-332, 2005.
26. G. Vernizzi, M. Lanzerotti, J. Kujawski, A. Weatherwax, "Topological constraints for E. F. Rent's work on micro miniature packaging and circuitry," *IBM Journal of Research and Development,* Paper 13, vol. 58, no. 2/3, March/May 2014.
27. L. A. Hsia, G. Vernizzi, M. Y. Lanzerotti, D. Langley, M. K. Seery and L. Orlando, "Topological constraints of gate-level circuits obtained through standard cell recognition (SCR)," *2015 National Aerospace and Electronics Conference (NAECON)*, Dayton, OH, 2015, pp. 165-175.
28. M. Lanzerotti, "System and method for identifying electrical properties of integrate circuits," U.S. Patent 9,230,050, Jan. 5, 2016.